

MULTIPLE REGISTRATION SYSTEM AND METHOD OF USING THE
SAME ACCOUNT FOR REGISTERING DIFFERENT DEVICES TO A DRC
SERVER

BACKGROUND OF THE INVENTION

5 This application incorporates by reference Provisional application Serial No.
89128086, Filed Dec. 28, 2000.

Field of the Invention

10 This invention relates to a system and a method of registration and usage of an
account, and more particularly to a system and a method capable of using the same
account for registering different devices to a DRC (Digital Right Certificate) server
through a network system.

Description of the Related Art

15 As the continuous improvement of computer technology, the applications of
computers and the network have not only been limited in delivering or sharing
information, but also gradually change commercial trading behaviors of consumers.
In the past, consumers had to go to a shopping center personally to choose goods and
proceed with a trade. As the fast development of computer network, consumers can
20 use the E-Commerce in the Internet to buy goods now. And the supplier will deliver

the sold goods to a consumer by a delivery company. In addition, a consumer can also use E-Commerce to buy a digital content, such as e-book, digital music such as MP3, or a system and software of computer application, and so on. A consumer can directly download the ordered digital content from the Internet. This trading method
5 seems to be very convenient and effective for both consumers and suppliers.

However, before the download process of the ordered digital content to the corresponding consumer, a supplier would proceed with encryption on the associated digital content in order to prevent illegal copy or unauthorized distribution. Afterwards, the supplier would then allow the download procedure by showing a
10 download manual to consumers. In this way, the supplier can prevent the consumer from using the downloaded digital content in another machine or device, and consequently can prevent the illegal copy or unauthorized distribution of the digital content. However, by doing so, the consumer's legal right and benefit would also be restricted a lot at the same time.

SUMMARY OF THE INVENTION

It is therefore an object of the invention to provide a system and a method of using the same account for multiple registrations in different devices. The present
20 invention enables a user to perform multiple registrations of the same account to a server in different devices. The downloaded digital content can therefore be legally

utilized in all the authorized devices, and not limited to only one single device.

However, at the same time, the present invention can still achieve the important goal of preventing illegal copy or distribution to unauthorized or unregistered devices.

The object of this invention is to provide a method of using the same account for multiple registrations indifferent devices. The method enables a user to proceed the registration procedure to a digital right certificate (DRC) server in a first device, in order to purchase and download a digital content through a network. In the first device, there is already a first reader or program installed for the user to open the downloaded digital content. The associated method of this invention firstly, at Step A, installs the first reader into the first device, then builds connection between the first reader and the DRC server through a network system, and begins the further registration procedure. At Step B, the DRC server generates a user identity (UID), encrypts the UID, and then transmits it to the first reader. At this step, the first reader further stores the UID and a first device identity code in an encrypted first right record file. Whenever necessary, the UID can be retrieved or read out through the first reader by the user. Then at Step C, the first reader transmits the first device identity code to the DRC server. The first right record file and the first device identity code therein help the identification process, and then decide whether to start decryption or not. That is, when the first reader is initiated to begin decryption, it checks if the first right record file has been changed, and then checks if the first device identity code in the first right record file is correct or not.

Then, a user can further use a second device to register to the DRC server by

using the aforementioned UID. The method of this invention further comprises step D: installing a second reader in the second device, and inputting the UID into the second reader. The second reader would then store the UID and a second device identity code in an encrypted second right record file. Furthermore, at step E, the second reader transmits the UID and the second device identity code to the DRC server. Finally, at Step F, the DRC server transmits all digital right coupons of the specific digital contents that the user purchased to the second reader. And the second reader stores the coupons in the second right record file.

The invention achieves the above-identified object by further providing a system for using the same account for multiple registrations in different devices. The system enables a user to use the same account in different devices and to purchase and download a digital content via a network. The system comprises a first device and a DRC server. The first device comprises a first reader and a first device identity code. The first device can build connection with the DRC server through the network. And the DRC server is aimed at providing and controlling the related registration procedures when the first device applies for an account or a user identity (UID). The aforementioned system uses the first reader to encrypt the UID and the first device identity code, and to store them into a first right record file, and then to transmit the UID and the first device identity code to the DRC server. The first right record file and the first device identity code therein help the identification process, and then decide whether to start decryption or not. That is, when the first reader is initiated to begin decryption, it first checks if the first right record file has been changed, and then check if the first device identity code in the first right record file is correct.

In addition, the system of the present invention further comprises a second device. The second device includes a second reader and a second device identity code. The second device builds connection with the DRC server through the network. The user, who wishes to apply multiple registrations, can then input the same UID into the second reader. The second reader encrypts and stores the UID and the second device identity code in a second right record file. And the second device identity code is also transmitted to the DRC server. The second right record file and the second device identity code therein also help the identification process, and then decide whether to start decryption or not. That is, when the second reader is initiated to begin decryption, it will firstly check if the second right record file has been changed, and then check if the second device identity code in the second right record file is correct or not.

BRIEF DESCRIPTION OF THE DRAWINGS

Objects, features, and advantages of the invention will become apparent from the following detailed description of the preferred but non-limiting embodiments. The description is made with reference to the accompanying drawings, in which:

Figure 1 is a system structure diagram of one preferred embodiment of the system capable of using the same account for multiple registrations in different devices

Figure 2 is a flow chart of the process steps for the first device in Figure 1 to

register to a DRC server and receive a user account.

Figure 3 is an illustration of content format of a digital right coupon corresponding to a digital content.

Figure 4 is a flow chart of the process steps for the second device in Figure 1 to use the same registration account in the first device to perform multiple registrations to the DRC server.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Please refer to Figure 1. Figure 1 is a system structure diagram of one preferred embodiment of the system of using the same account for multiple registrations in different devices. In Figure 1, the first device 101 and the second device 103 can build connections with a digital right certificate (DRC) server 107 through the network 105. The first device 101 and the second device 103 can either be a personal computer, a notebook, a laptop, a personal digital assistant (PDA), a smart phone, or a device capable of receiving or transmitting message through wired or wireless network. The DRC server 107 performs the functions of controlling, managing and maintaining user's registration data, the record and rights of the purchased digital contents by a user. The user can proceed the registration procedure to the DRC server 107 via the first device 101 or the second device 103.

The system of the present invention utilizes reader programs 111, 121 to perform multiple registrations of the same account in different devices 101, 103.

Please refer to Figure 2. Figure 2 is a flow chart of the process steps for the first device 101 in Figure 1 to register to a DRC server 107 and receive a user account. In Figure 2, at Step 201, it shows to install a reader 111 in the first device 101, and to build connection with the DRC server 107 to begin the registration process. The user can download the reader 111 from the DRC server 107 or related network shops and fill registration data. The registration data includes the user's name, age, address or other related information.

At Step 203, the DRC server 107 examines and checks the user's registration data. If the examination is passed and approved, the method proceeds to Step 205; otherwise, this method ends. At this step, the DRC server 107 also checks to see if the user's registration data is enough and correct.

At Step 205, after the registration is approved, the DRC server 107 generates a user's identity (UID) to represent the user's account for further identification. As shown in Figure 1, the DRC server 107 further comprises a digital right database 109. The DRC server 107 stores the UID in the digital right database 109. Then, the DRC server 107 transmits the UID to the reader 111. For securely delivering the UID through the network, the DRC server 107 encrypts UID and then transmits the UID to the reader 111. The reader 111 stores the UID and a device identity code 113 of the first device 101 in a rights record file 115, which is an encrypted file. It is possible for the user to retrieve or read out the exact value of UID through the reader 111, but the user has no way to change it. Besides, the device identity code 113 can be a serial number of a hard disk drive, an identified number of a CPU, a card number of a

network card or other unique serial number of hardware parts in the first device 101.

At Step 207, the reader 111 asks if the user agrees to transmit the device identity code 113 to the DRC server 107. It is done because of the privacy policy concern. If the user agrees, the method proceeds to Step 209, otherwise, the procedure is ended.

At Step 209, the reader 111 transmits the device identity code 113 to the DRC server 107. The DRC server 107 stores the device identity code 113 in the digital right database 109. When the aforementioned procedures are finished, the registration process of the first device 101 is completed.

Afterwards, the user can use the first device 101 to order and download a desired digital content. Before the desired digital content is downloaded, the server 107 that supplies downloadable digital contents uses a unique encryption key to encrypt this digital content. Then the encrypted digital content can be downloaded to the first device 101. There is an accompanied digital right coupon 110 in association with the corresponding digital content for recording the associated digital rights and related information for this particular UID to use the digital content. And the digital right coupon 110 is stored in the digital right database 109 of the DRC server 107. Please refer to Figure 3. Figure 3 is an illustration of content format of the digital right coupon 110. As shown in Figure 3, the content format of the digital right coupon 110 comprises at least the following fields: owner identity, serial number of digital content, allowable times for downloading, expiry date, password of encrypted

digital content.

The field for an owner identity of the digital right coupon 110 can be the UID of the corresponding user who purchases the digital content. The field of the serial number of a digital content is the unique serial number for this particular downloaded digital content. The field of allowable times for downloading is for recording times for the user to download this particular digital content. For example, when a user purchases a digital content with a right of 5 times download permission, then the value is 5. Afterwards, every time when the user uses a different device to download the digital content, this value would be subtracted one. If the user uses the same device to download the same digital content again, this value remains the same and would not change. And the field of expiry date is for recording the expiration date of the digital content wherein the user is authorized to use this digital content. The field of password of encrypted digital content is for recording a necessary password when the user uses the first reader to open the digital content. This password is corresponding to the encryption key to encrypt this particular digital content to be downloaded.

Then the first device 101 downloads an encrypted digital right coupon 110 in associated with the particular digital content and stores it into the right record file 113 in the first device 101.

The reader 111 further comprises a checking procedure. When the reader 111 is initiated to begin decrypting a digital content, it would start the checking procedure to see if the right record file 115 is an original file downloaded from a DRC server 107.

If the right record file 115 is fabricated or modified, the checking procedure would stop the normal execution of the reader 111. In addition, the reader 111 would also check the device identity code of the present device. If the present device code is different from the device identity code 113 already stored in the right record file 115, that means, the right record file 115 is copied from another device. Therefore, the reader 111 would not continue to perform the normal execution and then terminate.

After the right record file 115 is checked and the reader 111 is then to open a downloaded digital content, the reader 111 would still check the digital right coupon of the digital content in the right record file 115. This is for the examination of the expiry day thereon. If the digital right coupon of the digital content is expired, the reader 111 would not open the expired digital content. If the coupon is within the expiry date, the reader 111 would read the password of the encrypted digital content from the file of the password of encrypted digital content, and then perform decryption and open the encrypted digital content.

However, when a user tries to use or read the digital content in the second device 103 or other devices, that user needs to install a reader in that device first. And after registering that device to the DRC server 107, the user can then open the digital content. Please refer to the following description how the other devices are registered to the DRC server 107.

Please refer to Figure 4. Figure 4 illustrates a flow chart of the process steps for the second device 103 in Figure 1 to use the same registration account (UID) in the

first device 101 to perform multiple registrations to the DRC server 107. At Step 401, the user first installs a reader 121 in the second device 103, and inputs the same registration account UID into the reader 121. The UID can be retrieved and read out from the reader 111 in the first device 101, and the value of the UID can be inputted
5 into the reader 121. At this step, the reader 121 stores the UID and a device identity code 123 of the second device 103 in a right record file 125. The right record file 125 is an encrypted file. And the device identity code 123 can be a serial number of a hard disk drive, an identity number of a CPU, a card number of a network card or other unique serial number of hardware parts of the second device 103.

10 At Step 403, the reader 121 asks if the user agrees to transmit the device identity code 123 to the DRC server 107 in order to proceed the further registration. This is also done due to the privacy policy concern. If yes, then the method proceeds to Step 405. Otherwise, the registration procedure of the second device 103 is ended.

15 At Step 405, the reader 121 transmits the UID and the device identity code 123 to the DRC server 107. The DRC server 107 would store the device identity code 123 in the digital right database 109.

20 Afterwards, at Step 407, the DRC server 107 examines and checks the registration of the second device 103. If the DRC server 107 approves the registration of the second device 103, then the method proceeds to Step 309; otherwise, the registration procedure of the second device 103 is ended. During this

step, the DRC server 107 examines the rights of the user recognized as UID, by checking if the UID is still within its expiry date, and if the UID has the right for fetching the digital content in other different devices.

At Step 409, the DRC server 107 transmits all the digital right coupons of the associated digital contents, which the user purchased in the original register account of UID, to the second device 103. After the reader 121 receives these digital right coupons and stores them in the right record file 125, the second device 103 can download those purchased digital contents from the DRC server 107. Then the reader 121 checks the right record file 125 and opens the downloaded digital content. Basically, the processing principle of the reader 121 is the same as the aforementioned process of the reader 111 in the first device 101.

The present invention revealed by the above embodiments has two advantages.

(1) To protect the right of suppliers: the invention provides the function of avoiding illegally copy or distribution of a digital content. Because the reader in this invention would check user's identity, a device identity code and the password of an encrypted digital content when the reader opens a digital content. If there is any illegal copy, the digital content cannot be opened.

(2) To enhance the convenience of a user: the present invention enables a user, after purchasing and downloading a digital content, to use the digital content in different devices which previously have passed the registration approval and examination procedure. That means, the digital content is not limited to only one

single device usage, and at the same time not breaking the supplier's security policy.

While the invention has been described above, by way of example and in terms of a preferred embodiment, it is to be understood that the invention is not limited thereto. On the contrary, it is intended to cover various modifications and similar arrangements and procedures, and the scope of the appended claims therefore should be accorded the broadest interpretation so as to encompass all such modifications and similar arrangements and procedures.

5